Blockchain

Beheersing, controls & assurance

in ketens / ecosystemen

Ronald Koorn (Partner KPMG IT Assurance & Advisory)
Namens NOREA Kennisgroep Keteninformatiemanagement
10 mei 2023

NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

Agenda

Aanleiding / achtergrond:

- Kennisgroep Keteninformatiemanagement actief op terrein van ketenassurance
- Publicatie 'Audit Alert beheersing keteninformatisering zorgsector' (Publieke ML)
- Blockchain & Assurance: handreiking voor IT-auditor


Keteninformatiemanagement

Blockchaintechnologie dwingt tot versterking interne beheersing en integrale auditing

22 september 2020 René Matthijsse

Blockchain zal leiden tot een andere wijze van kijken naar de beheersing van risico's en de vastlegging en inrichting van processen. Auditors hebben een strategische rol gekregen en moeten hun visie geven op allerlei integrale thema's. Het is de vraag of de auditor zich voldoende bewust is van de risico's naarmate de samenwerking met ketenpartners intensiever wordt en de innovatie in technologie toeneemt. Blockchaintechnologie kent op zichzelf geen fundamentele verschillen met bekende technologieën, maar leidt wel tot serieuze consequenties op specifieke risicogebieden. Deze trend dwingt tot de doorontwikkeling van audit en andere assuranceproducten in de richting van integrale auditing.

Achtergrond

Permisse: een blockchain-oplossing of andere gedistribueerde database met een multiparty consensusmodel kan effectief worden ingezet bij het managen van processen over organisatiegrenzen heen

→ Veelal ketenproces met zware administratieve component, met meerdere partijen, gezamenlijk belang ('dominant ketenprobleem'), informatie-assymetrie en hoog jaarlijks transactievolume

Hoe het begon in 2008

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

CRYPTOGRAFIE

Waardetransfer via internet

PEER-TO-PEER NETWERK

Zonder centrale partij (TTP)

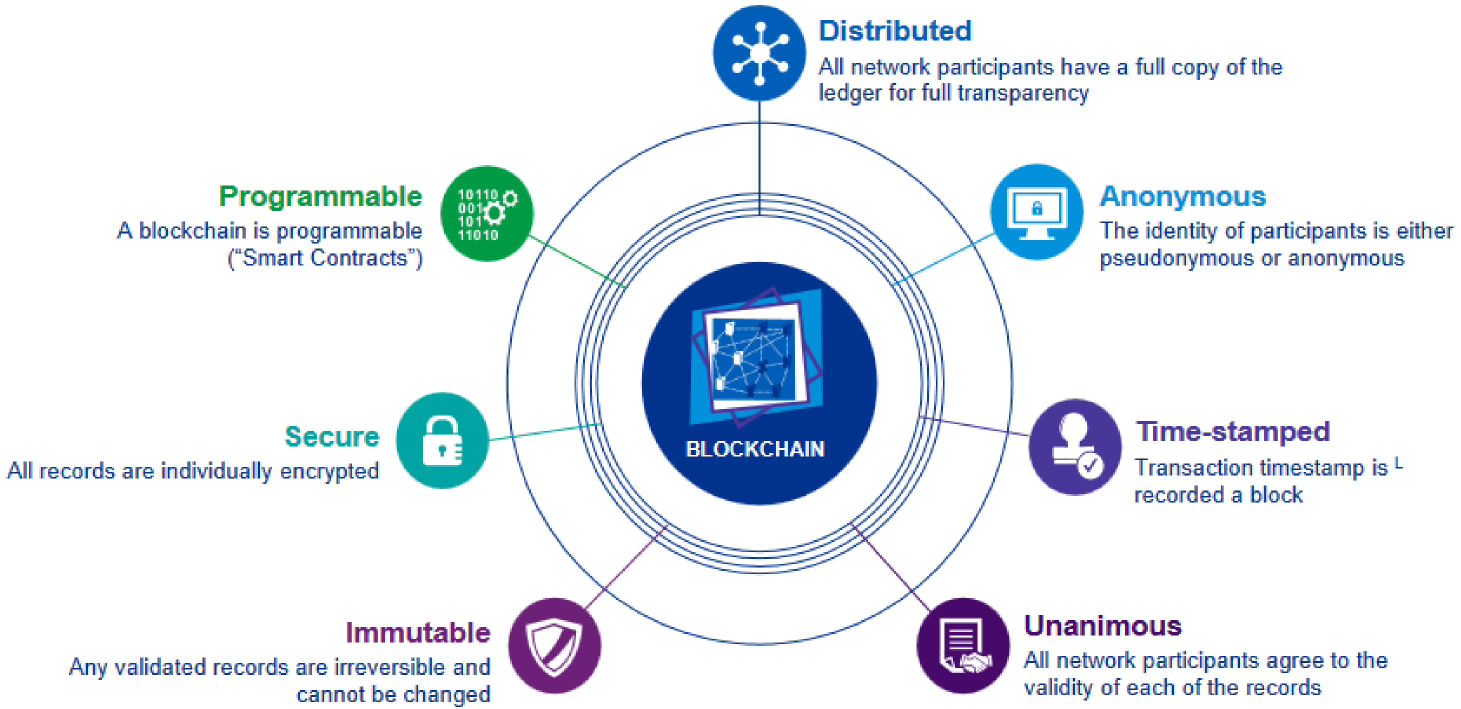
CONSENSUS-MECHANISME

Validatie door nodes in netwerk

DECENTRALE LEDGER

complete transparentie

Belangrijkste kenmerken



Bron: KPMG Research, 2021

Aanpak van onderzoek

- Opstellen van globaal raamwerk voor interviews / verwerking
- Uitwerking van 5 use cases, in sectoren:

  Mobiliteit, Transport, Tuinbouw, Bancair en Afvalverwerking
- Expertinterviews
- Opstellen van Handreiking

Blockchain: kans én bedreiging voor auditor

Dit onderzoek is uitgevoerd door de volgende Kennisgroepleden:

- dr. René Matthijsse RE
- drs. Youetta de Jager
- drs. ing. Ronald Koorn CISA RE
- Ruurd Smildiger RE
- Ruud Mollema RE
- drs. Reza Torabkhani RE
- Patrick Chu RE
- drs. Lucas Vousten RE
- drs. Marc Welters RA RE
- drs.ing. Michel Bernsen RE
- m.m.v. drs. Christel Maas……… en vele externe gesprekspartners

Agenda

01 Aanleiding

02 Welke aanpak?

03 Welke use cases zijn geanalyseerd?

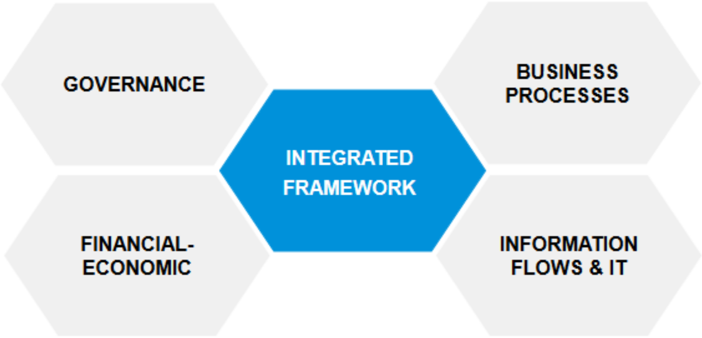
04 Is Blockchain Control Framework nodig?

05 Wat is opgevallen?

06 Hoe verder?

07 Q&A

NOREA Blockchain Control Framework



Audit domein	Control doelstelling	Risico ID	Risico-Gebied	Beheers-maatregel	Korte omschrijving
Governance Domein					
Financieel domein					
Processen domein					
IV-IT domein					

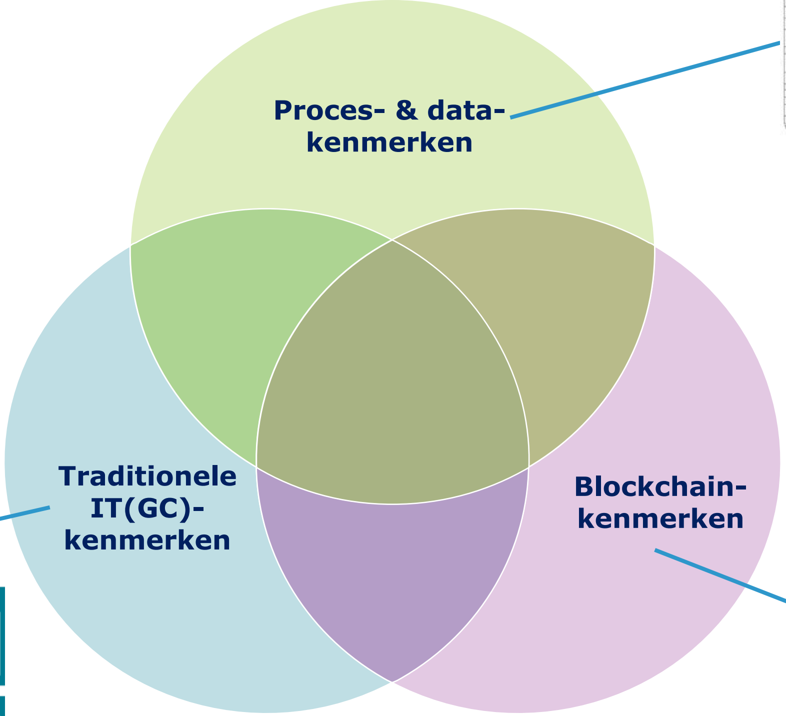
Governance domain
- Strategic objectives
- Governance & management
- Legislation & regulation
- Organisational setup

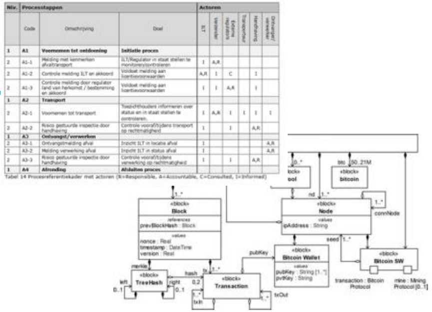
Financial domain
- Financial-economic objectives

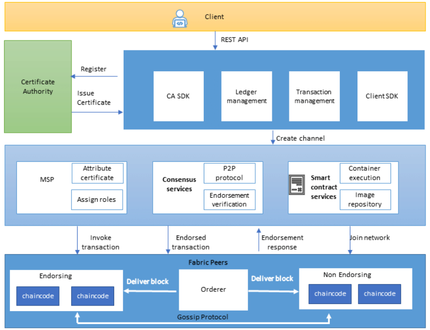
Process domain
- Business processes
- Social-organisational processes
- Marketing & Communication

IV-IT domain
- Data Management & data architecture
- Interconnectivity
- Data Privacy & Security
- Cryptographic key management
- Smart contracts
- Centralization & Collusion
- Interoperability & Integration
- Scalability & Continuity
- Platform standardisation & Migration

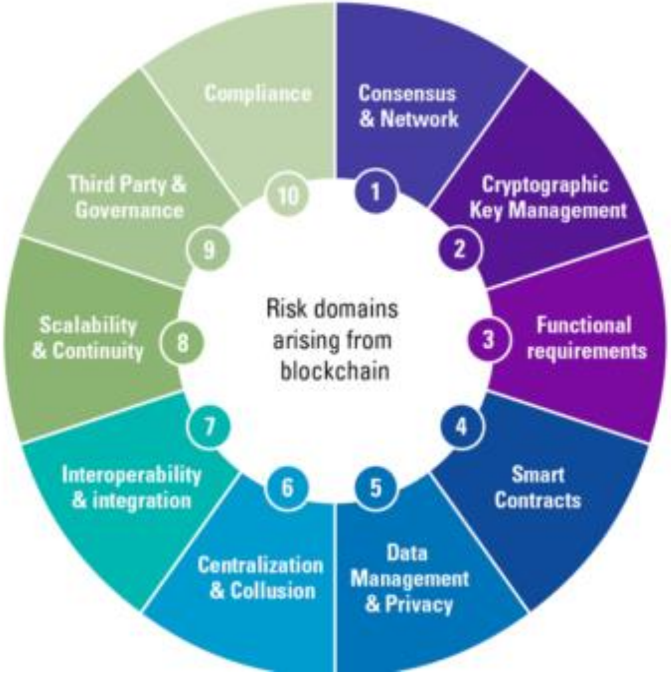
Domeinen auditscope







Blockchain-audit omvat meer dan IT- en harde controls



Construct: Data management				
Risk	**ID**	**Maturity self-assessment questionnaire**	**Maturity level**	**Literature**
Date used within the DLT is invalid or not accurate. Data is modified, inserted or deleted inappropriately	4.1.1	Integrity verification procedures are described;	If yes: maturity level 2	(Robeco: Jeroen van Oerle & Lemmens, 2016); (Tas ca et al., n.d.) (Morabito, 2017; Trautman, 2016) (Rights, 2017 (Hard y et al., 2008; ISACA, 2017; ITIL, 2013; NIST, 2016; OWASP, 2008))
	4.1.2	History of data in the DLT is immutable.	If yes: maturity level 3	
	4.1.3	Error checking mechanisms are in place to check entered data, such as input validation (completeness checks) to preclude the entering of invalid data, erro detection/data validation to identify errors in data	If yes: maturity level 3	
	4.1.4	Controls are in place, as conditions to be verified before data is updated.	If yes: maturity level 3	
	4.1.5	An assessment has been performed to the implementaton and security of used oracles by the DLT.	If yes: maturity level 3	
	4.1.6	Real world objects tracked in the DLT are on boarded by trusted party.	If yes: maturity level 3	
	4.1.7	A checkpointing system is implemented in the DLT to ensure data availability.	If yes: maturity level 3	
	4.1.8	A monitoring system is in place to verify the data integrity of underlying data sources connected to the DLT.	If yes: maturity level 4	

Voornaamste risicogebieden

- Authenticatie & autorisaties (IAM)
- Interoperabiliteit
- API’s / interfacing
- Datakwaliteit / datamanagement
- Change management (agile, smart contracts, testen)
- Privacy & compliance (internationaal)
- Schaalbaarheid & performance
- Kosten (project – operationeel)
- (Lange-termijn) continuïteit

Agenda

01 Aanleiding

02 Welke aanpak?

03 Welke use cases zijn geanalyseerd?

04 Is Blockchain Control Framework nodig?

05 Wat is opgevallen?

06 Hoe verder?

07 Q&A

Samenvattend: terug naar aanleiding van onderzoek Kennisgroep

- Blockchain-technologie verschilt niet fundamenteel met andere technologiën, wel tot serieuze consequenties op andere risicogebieden

- Organisatie & inrichting aangepaste beheersings-maatregelen spelen grotere rol spelen dan technologie

- Onderscheid control- vs. trust-benadering, ook bij besloten (permissioned) blockchain netwerken

Samenvattend: wat is opgevallen?

- Impact: technologisch & organisatorisch
- Governance: samenwerking – concurrentie, rollen – belangen (‘wie betaalt, die bepaalt’)
- Architectuur: toenemend gebruik standaardprotocollen/bouwblokken
- Data: inter-organisatorisch (master) data management
- Praktijktoepassing: veelal pilots, opschalen/on-boarding complex
- Beheersing: belang risicomanagement in keten/ecosysteem & ontbreken control frameworks
- Financieel: startfinanciering, kosten/baten(ver)deling/verrekening
- Zekerheid: ontbreken IT-assurance DLT-producten / veel impliciet vertrouwen in partijen
- Audit–trails: specifieke tooling
- Auditing: multidisciplinair auditteam / pooled audits / niet louter ITGC- of security-audit

Paradoxen & dilemma's

- Decentrale governance vs. centrale sturing & financiering
- Ongereguleerde (crypto) ecosystemen vs. compliance-vereisten aan blockchains
- Non-permissive blockchains hebben hoog energieverbruik vs. permissive blockchains vergen veel menselijke energie
- Blockchain kan functioneren zonder wederzijds vertrouwen vs. vertrouwen is cruciale substituut voor (harde) controls

Hoe verder als Kennisgroep?

- Afronden publicatie (plus uitdragen via ‘roadshow’)
- Uitwerken volledig Blockchain Control Framework en/of Blockchain risicoanalyse-methode?
- Uitvoeren specifieke blockchain audit o.b.v. BCF ?
- Toespitsen op cryptocurrencies / digitale euro ?
- Terug naar de basis: ketenbeheersing & ketenassurance
- Andere suggesties ?

Q&A

Voor meer informatie:

Christel Maas
c.maas@norea.nl

René Matthijsse

matthijsse.rene@gmail.com

Ronald Koorn

koorn.ronald@kpmg.nl

NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS